



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/774,079

02/06/2004

Shehzad T. Merchant

2717P176

7139

8791

7590

09/06/2011

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER

POPHAM, JEFFREY D

ART UNIT

PAPER NUMBER

2491

MAIL DATE

DELIVERY MODE

09/06/2011

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/774,079	Applicant(s) MERCHANT ET AL.	
	Examiner JEFFREY D. POPHAM	Art Unit 2491	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 June 2011.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on ____; the restriction requirement and election have been incorporated into this action.
- 4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 5) ☒ Claim(s) 1,4-7,10,14-16,19,20,24-26,39-43,46,48-50 and 54-56 is/are pending in the application.
- 5a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 6) ☐ Claim(s) ____ is/are allowed.
- 7) ☒ Claim(s) 1,4-7,10,14-16,19,20,24-26,39-43,46,48-50 and 54-56 is/are rejected.
- 8) ☐ Claim(s) ____ is/are objected to.
- 9) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 10) ☐ The specification is objected to by the Examiner.
- 11) ☒ The drawing(s) filed on 28 July 2009 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 12) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. ____. |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date ____. | 6) <input type="checkbox"/> Other: ____. |

Remarks

Claims 1, 4-7, 10, 14-16, 19-20, 24-26, 39-43, 46, 48-50, and 54-56 are pending.

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.

Applicant's submission filed on 6/16/2011 has been entered.

Response to Arguments

2. Applicant's arguments filed 6/16/2011 have been fully considered but they are not fully persuasive.

Applicant argues that the combination of identities of a user and of a mobile client of the user is not found in the cited references. However, Stewart discloses identities, such as MAC addresses, SIDs, and the like. Stewart refers to "credentials of the user" and that the PCD "of a first user comprises identification information having an access level...". Therefore, Stewart teaches an identity of the user's mobile client (PCD), and that this identity is associated with the user. As Stewart is not clear on the identity of the user being a username or the like, which is believed to be the intended identity of the user (e.g. new claims 54-56), Short is additionally cited below as providing the

Art Unit: 2491

combination of identities that are specifically of the user (e.g. user name or ID) and of the mobile client (e.g. circuit ID or MAC address) as seen in column 8, lines 10-14, for example.

Applicant's arguments with respect to the periodic downloading at regular intervals have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1, 4-6, 39-42, 46, 54, and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart (U.S. Patent 6,732,176) in view of Genty (U.S. Patent 7,496,755), Short (U.S. Patent 7,194,554), and Gage (U.S. Patent Application Publication 2002/0068584).

Regarding Claim 1,

Stewart discloses a method of controlling access to a network, the method comprising:

Configuring an authentication server to include a first location information corresponding to a combination of identities of a user and of a mobile client of the user (Column 2, lines 30-40;

Art Unit: 2491

Column 6, lines 15-28; Column 10, lines 8-15; Column 10, lines 38-63; and Column 11, lines 54-65; identification information include a combination of identities, such as SID and MAC IDs. As noted above, while the identities are associated with the user, Short is additionally cited below as more explicitly teaching an identity of a user being a user name. These citations will not be referred to every instance of the combination identities is mentioned, so as to more clearly and concisely provide pertinent citations for each particular limitation and such citations are hereby implicitly cited whenever such a combination of identities are referred to, as they define the combination of identities that makes up the identification information of Stewart), the first location information being a location at which the mobile client is permitted to connect to the network (Column 11, lines 28-53; and Column 16, lines 38-64; storing information regarding special locations, for example. In addition, U.S. Patent 5,835,061, incorporate by reference in column 4, lines 39-43, includes additional information regarding storing of locations);

Requesting by a network switch the combination of identities of the user and of the mobile client of the user attempting to connect to the network (Column 10, line 64 to Column 11, line 16; request for identification information, for example);

Receiving, by the authentication server, the combination of identities of the user and of the mobile client of the user via the network switch (Column 11, lines 17-53);

Associating, by the network switch, a second location information corresponding to the mobile client with the combination of identities of the user and of the mobile client of the user, wherein the second location information indicates a location of the network switch coupled to the network to which the mobile client is attempting to connect (Column 8, lines 17-33; Column 11, lines 17-53; and Column 16, lines 38-64; associating the client's current location with the client, where the client's location can be that of the AP to which the client is connecting, for example);

Storing the second location information on the network switch (Column 7, line 62 to Column 8, line 3; Column 11, lines 28-53; and Column 16, lines 38-64);

Authenticating, by the authentication server, the combination of identities of the user and of the mobile client of the user received by the authentication server (Column 9, lines 28-47; Column 12, line 30 to Column 13, line 10; and Column 18, lines 1-25);

Comparing, by the authentication server, the second location information corresponding to the mobile client against the first location information (Column 11, lines 28-53; and Column 16, lines

38-64; determining access levels based on current location compared to stored locations, for example);

Deciding, by the authentication server, whether to grant or deny access to the network for the mobile client in response to authenticating the combination of the identities of the user and of the mobile client of the user, wherein the deciding is in response to comparing the second location information against the first location information (Column 11, lines 28-53; Column 12, lines 47-63; and Column 16, lines 15-55; granting differing levels of access based on identification information as well as geographic information, for example); and

Informing the network switch by the authentication server whether to grant or deny access to the network for the mobile client (Figure 4, 224, 226, 232; and Column 11, lines 28-53; Column 12, lines 47-63; and Column 16, lines 15-55; allowing or disallowing access based on identification, geographic information, and the like, for example);

But does not explicitly disclose that the authentication server is coupled to the network and comprises a RADIUS server having RADIUS attributes; that the first location information is included within a RADIUS VSA of the RADIUS attributes; or periodically downloading at regular intervals the stored second location

information to an edge device, wherein the mobile client is operable to connect to the network via the edge device.

Genty, however, discloses that the authentication server is coupled to the network and comprises a RADIUS server having RADIUS attributes (Abstract; Column 12, lines 30-44; and Column 14, lines 27-45; RADIUS server with RADIUS attributes, for example), and

That RADIUS can be extended to attributes not defined in RADIUS by a vendor by use of vendor specific attributes (VSAs) (Column 12, lines 30-44). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication techniques of Genty into the distributed network access system of Stewart in order to allow the system to easily specify any information required within the authentication server or corresponding database by use of an extensible attribute set, thereby allowing additional types of information to be stored for authentication purposes even after the system has been deployed.

Short, however, discloses that the combination of identities includes an identity of a user and of a mobile client of the user (Column 8, lines 10-32; username and MAC address, as examples);

That the extended attribute (stored in the VSA in the combination) is the first location information and that the first location information used in comparison is taken from the extended attribute (Column 7, line 41 to Column 8, line 32; and Column 10, lines 9-63; storing locations in the profile, which can store RADIUS information, for example). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the profile-based authorization system of Short into the distributed network access system of Stewart as modified by Genty in order to allow the system to verify a variety of information such as location, device, user, time, location status, etc. with respect to the client's profile prior to authorizing access, thereby providing fine-grained access control.

Gage, however, discloses periodically downloading at regular intervals the stored second location information to an edge device, wherein the mobile client is operable to connect to the network via the edge device (Paragraphs 52, 54, 63-64, and 84; location report being issued periodically from the client to the location update unit or to the radio edge routers, which then sends this location report to the network edge routers, resulting in the mobile device's location being periodically sent from the location update unit (described as being a switch in paragraph 52) to the routers, where the client is operably connected to the routers, since

Art Unit: 2491

the routers send and receive information to and from the mobile clients, for example). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the location updating and mapping techniques of Gage into the distributed network access system of Stewart as modified by Genty and Short in order to allow the system to more efficiently transmit data, since each router will know the current location of each mobile device, thereby allowing each router to transmit data for the device to the correct next-step router, resulting in faster communication and higher efficiency in routing.

Regarding Claim 39,

Claim 39 is a system claim that corresponds to method claim 1 and is rejected for the same reasons.

Regarding Claim 4,

Stewart as modified by Genty, Short, and Gage discloses the method of claim 1, in addition, Stewart discloses that the identity of the mobile client includes information selected from the group consisting of a user name, a user password, a certificate, a MAC address, a shared encryption key, a smart card identifier, and any combination of the foregoing information (Column 10, lines 53-63).

Regarding Claim 40,

Claim 40 is a system claim that corresponds to method claim 4 and is rejected for the same reasons.

Regarding Claim 5,

Stewart as modified by Genty, Short, and Gage discloses the method of claim 1, in addition, Stewart discloses that the edge device is capable of providing one or more wireless devices an access point for connecting to the network (Column 10, line 64 to Column 11, line 16); and Gage discloses that the edge device is capable of providing one or more wireless devices an access point for connecting to the network (Paragraphs 52, 54, 63-64, and 84).

Regarding Claim 41,

Claim 41 is a system claim that corresponds to method claim 5 and is rejected for the same reasons.

Regarding Claim 6,

Stewart as modified by Genty, Short, and Gage discloses the method of claim 1, in addition, Stewart discloses that the mobile client is a wired device capable of connecting to the network through an Ethernet switch port (Column 5, lines 2-24; Column 6, lines 40-59; and Column 9, lines 48-64).

Regarding Claim 42,

Claim 42 is a system claim that corresponds to method claim 6 and is rejected for the same reasons.

Regarding Claim 46,

Stewart as modified by Genty, Short, and Gage discloses the method of claim 1, in addition, Stewart discloses that the mobile client is associated with a newly located access point upon authenticating the combination of identities of the user station and of the mobile client and determining, by comparing an updated location information corresponding to the mobile client against the first location information in the policy table, the first location information being the information that the mobile client is still authorized to access the network (Column 9, lines 28-47; Column 10, lines 25-37; Column 12, line 30 to Column 13, line 10; Column 14, line 57 to Column 15, line 15; and Column 18, lines 1-25).

Regarding Claim 54,

Stewart as modified by Genty, Short, and Gage discloses the method of claim 1, in addition, Short discloses that the user identity comprises user name (Column 8, lines 10-32).

Regarding Claim 56,

Claim 56 is a system claim that corresponds to method claim 54 and is rejected for the same reasons.

4. Claims 7 and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Genty, Short, and Gage, further in view of Funk (Funk Software, "Comprehensive RADIUS/AAA Solution for the Global Enterprise", 2/22/2003, pp. 1-6).

Regarding Claim 7,

Stewart as modified by Genty, Short, and Gage discloses that the identity comprises a combination of identities of the user and of the mobile client of the user (Short, Column 8, lines 10-32, for example), but does not explicitly disclose that authenticating the combination of identities of the user station and of the mobile client comprises authenticating the identity of the mobile client via a mechanism selected from the group comprising TLS, TTLS, MD5, EAP-TLS, and any combination of the foregoing.

Funk, however, discloses that authenticating the identity of the mobile client comprises authenticating the identity of the mobile client via a mechanism selected from the group comprising TLS, TTLS, MD5, EAP-TLS, and any combination of the foregoing (Page 3). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the AAA system of Funk into the distributed network access system of Stewart as modified by Genty, Short, and Gage in order to allow the system to authenticate via a wide array of authentication mechanisms, and/or to provide high reliability and uptime.

Regarding Claim 43,

Claim 43 is a system claim that is broader than method claim 7 and is rejected for the same reasons.

Art Unit: 2491

5. Claim 48 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Genty, Short, and Gage, further in view of Liming (U.S. Patent Application Publication 2002/0055924).

Stewart as modified by Genty, Short, and Gage does not explicitly disclose that the second location information indicates a location of a port of the network switch to which the mobile client is attempting to connect.

Liming, however, discloses that the second location information indicates a location of a port of the network switch to which the mobile client is attempting to connect (Paragraphs 159, 165, and 181). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the location context system of Liming into the distributed network access system of Stewart as modified by Genty, Short, and Gage in order to allow the system to associate location information with the client even when the other devices cannot provide such location information, thereby extending the system to be able to be used when the client connects directly to a switch and/or when the other devices between the client and switch do not have any means to associate location information with the client.

6. Claims 10, 14-16, 19, 24, and 55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Genty, Short, Gage, and Torvinen (U.S. Patent Application Publication 2005/0149443).

Regarding Claim 10,

Stewart discloses a network system comprising:

A network (Figure 1);

An authentication server coupled to the network, the authentication server configured to include a first location information corresponding to a combination of identities of a user and of a mobile client of the user (Column 2, lines 30-40; Column 6, lines 15-28; Column 10, lines 8-15; Column 10, lines 38-63; and Column 11, lines 54-65), the first location information being a location at which the mobile client is permitted to connect to the network (Column 11, lines 28-53; and Column 16, lines 38-64);

A network switch coupled to the network and having an authenticator for requesting a combination of identities of the user and of a mobile client of the user and for associating a second location information corresponding to the mobile client with the combination of identities of the user and of a mobile client of the user, wherein the mobile client is operable to communicate to the authenticator of the network switch, and wherein the second location information indicates a location of the network switch coupled to the network to which the mobile client is attempting to connect (Column 8, lines 17-33; Column 10, line 64 to Column 11, line 53; and Column 16, lines 38-64); and

A network manager operable to store the second location information on the network switch (Column 7, line 62 to Column 8, line 3; Column 11, lines 28-53; and Column 16, lines 38-64);

Wherein the authentication server is operable to:

Authenticate the combination of identities of the user and of a mobile client of the user received by the authentication server (Column 9, lines 28-47; Column 12, line 30 to Column 13, line 10; and Column 18, lines 1-25);

Compare the second location information corresponding to the mobile client against the first location information (Column 11, lines 28-53; and Column 16, lines 38-64);

Decide whether to grant or deny access to the network for the mobile client in response to authenticating the combination of identities of the user and of a mobile client of the user and in response to comparing the second location information against the first location information (Column 11, lines 28-53; Column 12, lines 47-63; and Column 16, lines 15-55); and

Inform the network switch whether to grant or deny access to the network for the mobile client (Figure 4; 224, 226, 232; Column 11, lines 28-53; Column 12, lines 47-63; and Column 16, lines 15-55);

But does not explicitly disclose that the authentication server comprises a RADIUS server having RADIUS attributes; that the first

location information is included within a RADIUS VSA of the RADIUS attributes; or that the network manager comprises an application running on a server, wherein the application permits a network administrator to create and update a policy table of the authentication server, wherein the network manager is operable to periodically download at regular intervals the stored second location information to an edge device, wherein the mobile client is operable to connect to the network via the edge device.

Genty, however, discloses that the authentication server is coupled to the network and comprises a Remote Authentication Dial-In User Service (RADIUS) server having RADIUS attributes (Abstract; Column 12, lines 30-44; and Column 14, lines 27-45); and

That RADIUS can be extended to attributes not defined in RADIUS by a vendor by use of vendor specific attributes (VSAs) (Column 12, lines 30-44). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication techniques of Genty into the distributed network access system of Stewart in order to allow the system to easily specify any information required within the authentication server or corresponding database by use of an extensible attribute set, thereby allowing additional types of

information to be stored for authentication purposes even after the system has been deployed.

Short, however, discloses that the combination of identities includes an identity of a user and of a mobile client of the user (Column 8, lines 10-32);

That the extended attribute (stored in the VSA in the combination) is the first location information and that the first location information used in comparison is taken from the extended attribute (Column 7, line 41 to Column 8, line 32; and Column 10, lines 9-63). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the profile-based authorization system of Short into the distributed network access system of Stewart as modified by Genty in order to allow the system to verify a variety of information such as location, device, user, time, location status, etc. with respect to the client's profile prior to authorizing access, thereby providing fine-grained access control.

Gage, however, discloses that the network manager is operable to periodically download at regular intervals the stored second location information to an edge device, wherein the mobile client is operable to connect to the network via the edge device (Paragraphs 52, 54, 63-64, and 84). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to

incorporate the location updating and mapping techniques of Gage into the distributed network access system of Stewart as modified by Genty and Short in order to allow the system to more efficiently transmit data, since each router will know the current location of each mobile device, thereby allowing each router to transmit data for the device to the correct next-step router, resulting in faster communication and higher efficiency in routing.

Torvinen, however, discloses that the network manager comprises an application running on a server, wherein the application permits a network administrator to create and update a policy table of the authentication server (Paragraphs 27-28, 30, 42, 45, 54, and 58; a management component, logic, or application that allows a network operator or user in control of a group to create and maintain a data structure including a region of interest and/or proficiency level that is allowed to join the group in order to perform particular actions or acquire particular data associated with the group, for example). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the conditional group access system of Torvinen into the distributed network access system of Stewart as modified by Genty, Short, and Gage in order to allow various groups to be formed, by network operators and normal users alike, such that groups may be based upon the location of the device, device capabilities, user capabilities

or subscriptions, etc., thereby providing additional beneficial services to users by allowing them to communicate with other users that are in the same location and/or have the same interests.

Regarding Claim 14,

Stewart as modified by Genty, Short, Gage, and Torvinen discloses the system of claim 13, in addition, Stewart discloses that the edge device is a wireless access point (Column 10, line 64 to Column 11, line 16).

Regarding Claim 15,

Stewart as modified by Genty, Short, Gage, and Torvinen discloses the system of claim 14, in addition, Stewart discloses that the mobile client is capable of connecting to the network through the wireless access point of the edge device (Column 5, lines 1-14; and Column 10, line 64 to Column 11, line 16); and Gage discloses that the mobile client is capable of connecting to the network through the wireless access point of the edge device (Paragraphs 52, 54, 63-64, and 84).

Regarding Claim 16,

Stewart as modified by Genty, Short, Gage, and Torvinen discloses the system of claim 10, in addition, Stewart discloses that the mobile client is a wired device capable of connecting to the network switch through an Ethernet port (Column 5, lines 2-24; Column 6, lines 40-59; and Column 9, lines 48-64).

Regarding Claim 19,

Stewart as modified by Genty, Short, Gage, and Torvinen discloses the system of claim 10, in addition, Torvinen discloses an interface for permitting an administrator to associate the second location information to the mobile client (Paragraphs 27-28, 30, 40, 42, 45, 54, and 58; associating the location-based group with mobile clients, for example).

Regarding Claim 24,

Stewart as modified by Genty, Short, Gage, and Torvinen discloses the system of claim 10, in addition, Stewart discloses that the identity of the mobile client includes information selected from the group consisting of a user name, a user password, a certificate, a MAC address, a shared key, a smart card identifier, and any combination of the foregoing information (Column 10, lines 53-63).

Regarding Claim 55,

Stewart as modified by Genty, Short, Gage, and Torvinen discloses the system of claim 10, in addition, Short discloses that the user identity comprises user name (Column 8, lines 10-32).

7. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Genty, Short, Gage, and Torvinen, further in view of Kwan (U.S. Patent Application Publication 2004/0255154).

Stewart as modified by Genty, Short, Gage, and Torvinen does not explicitly disclose that the authentication server is included in a network switch.

Kwan, however, discloses that the authentication server is included in a network switch (Paragraph 36). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the multi-tiered network security system of Kwan into the distributed network access system of Stewart as modified by Genty, Short, Gage, and Torvinen in order to ensure that a client and its associated user are authentic and authorized to use the system by three levels of security checks, including physical address authentication of the device, user credential authentication, and VLAN group association checks, thereby increasing security of the system.

8. Claims 25 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Genty, Short, Gage, and Torvinen further in view of Funk.

Regarding Claim 25,

Stewart as modified by Genty, Short, Gage, and Torvinen does not explicitly disclose that the network switch comprises an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.

Funk, however, discloses that the network switch comprises an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing (Page 3). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the AAA system of Funk into the distributed network access system of Stewart as modified by Genty, Short, Gage, and Torvinen in order to allow the system to authenticate via a wide array of authentication mechanisms, and/or to provide high reliability and uptime.

Regarding Claim 26,

Stewart as modified by Genty, Short, Gage, and Torvinen does not explicitly disclose that the authentication server comprises an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing.

Funk, however, discloses that the authentication server comprises an authentication mechanism selected from the group consisting of TLS, TTLS, MD5, EAP-TTLS, EAP-TLS, and any combination of the foregoing (Page 3). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the AAA system of Funk into the distributed network access system of Stewart as modified by Genty, Short, Gage, and

Torvinen in order to allow the system to authenticate via a wide array of authentication mechanisms, and/or to provide high reliability and uptime.

9. Claim 49 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Genty, Short, Gage, and Torvinen, further in view of Liming.

Stewart as modified by Genty, Short, Gage, and Torvinen does not explicitly disclose that the second location information indicates a location of a port of the network switch to which the mobile client is attempting to connect.

Liming, however, discloses that the second location information indicates a location of a port of the network switch to which the mobile client is attempting to connect (Paragraphs 159, 165, and 181). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the location context system of Liming into the distributed network access system of Stewart as modified by Genty, Short, Gage, and Torvinen in order to allow the system to associate location information with the client even when the other devices cannot provide such location information, thereby extending the system to be able to be used when the client connects directly to a switch and/or when the other devices between the client and switch do not have any means to associate location information with the client.

Art Unit: 2491

10. Claim 50 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Genty, Short, Gage, and Torvinen, further in view of Tan (U.S. Patent Application Publication 2001/0045451).

Stewart as modified by Genty, Short, Gage, and Torvinen does not explicitly disclose that the identity of the mobile client includes a smart card identifier.

Tan, however, discloses that the identity of the mobile client includes a smart card identifier (Paragraphs 20-23). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the smart card-based authentication techniques of Tan into the distributed network access system of Stewart as modified by Genty, Short, Gage, and Torvinen in order to provide multiple factor authentication, such that the user must first authenticate to the smart card, which will then allow the smart card to authenticate with the authentication server in a much more secure manner than simply by sending a username and/or password to the server for authentication.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ashok Patel can be reached on (571)272-3972. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JEFFREY D POPHAM
Primary Examiner
Art Unit 2491

/JEFFREY D POPHAM/
Primary Examiner, Art Unit 2491